

(19) 日本国特許庁(JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 10 - 333839

(43) 公開日 平成10年(1998)12月18日

(51) Int. Cl. <sup>6</sup>	識別記号	F I
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06 3 0 4 H
	5 4 0	5 4 0
12/14	3 2 0	12/14 3 2 0 F
H 0 4 L 12/56		H 0 4 L 11/20 1 0 2 A
12/22		11/26
審査請求 未請求 請求項の数9	O L	(全 1 2 頁)

(21) 出願番号 特願平9-140029

(22) 出願日 平成9年(1997)5月29日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 眞田 明美

神奈川県小田原市国府津2880番地株式会社

日立製作所ストレージシステム事業部内

(72) 発明者 中野 俊夫

神奈川県小田原市国府津2880番地株式会社

日立製作所ストレージシステム事業部内

(72) 発明者 岩崎 秀彦

神奈川県小田原市国府津2880番地株式会社

日立製作所ストレージシステム事業部内

(74) 代理人 弁理士 高橋 明夫 (外1名)

最終頁に続く

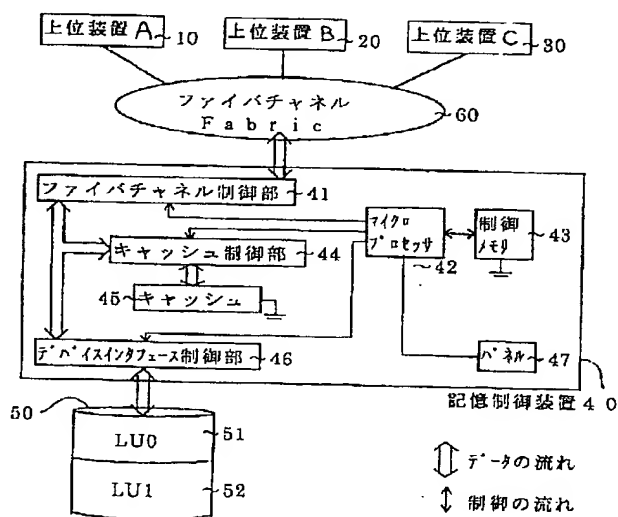
(54) 【発明の名称】 ファイバチャネル接続記憶制御装置

(57) 【要約】

【課題】 物理的にあらゆる上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを防止するセキュリティ機能を持つファイバチャネル接続記憶制御装置を提供する。

【解決手段】 上位装置を一意に識別できるN\_Port\_Name情報を、上位装置10、20、30の立ち上がる以前に、記憶制御装置40のマイクロプロセッサ42に設定しておき、上位装置10、20、30が立ち上がり、発行したフレームを記憶制御装置40が受領した際、マイクロプロセッサ42は、当該フレームに格納されているN\_Port\_Name情報が当該マイクロプロセッサ42に既に設定され、保持されている制御テーブル内のN\_Port\_Nameリストに登録されているかどうか、比較を行い、一致した場合は当該フレームの指示に基づく処理を継続し、不一致の場合は要求を拒絶する。これにより、上位装置からの不正アクセスを抑止することができ、セキュリティが保持できる。

図 1



## 【特許請求の範囲】

【請求項1】ANSIX3T11で標準化されたファイバチャンネルを、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び、記憶制御装置配下の磁気ディスクドライブで構成された記憶装置から成るコンピュータシステムにおいて、

上位装置から発行される、上位装置を一意に識別する情報であるN\_Port\_Name情報を、上位装置の立ち上がる以前に記憶制御装置に設置しておき、記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有し、上位装置が立ち上がった後、上位装置が、N\_Port\_Name情報を格納したフレームを記憶制御装置に対して発行し、記憶制御装置がこれを受領した際、既に設定され、保持されている上位装置を一意に識別するN\_Port\_Name情報と、受領したフレームに格納されたN\_Port\_Name情報とを比較する手段を有し、比較により一致した場合、当該フレームの指示に基づく処理を継続し、不一致の場合、受領した当該フレームを拒絶するLS\_RJT(Link Service Reject)フレームを上位装置に返し、上位装置からの不正アクセスを抑止する手段を有することを特徴とするファイバチャンネル接続記憶制御装置。

【請求項2】請求項1記載のファイバチャンネル接続記憶制御装置において、

当該記憶制御装置が有する上位インタフェース（ポート）の物理的な数以上のN\_Port\_Name情報を設定する手段、すなわち1ポートで複数のN\_Port\_Name情報を設定する手段を有し、ファイバチャンネルFabric接続時の論理パス多重構成にも上位装置からの不正アクセスを抑止する手段を有することを特徴とするファイバチャンネル接続記憶制御装置。

【請求項3】請求項2記載のファイバチャンネル接続記憶制御装置において、

当該記憶制御装置の配下にディスクアレイ装置のように多くの磁気ディスクボリュームを有し、複数のチャンネルパスルートを有するシステムにおいて、LUN（ロジカルユニットナンバ）による論理ディスク領域、RAIDグループによる論理ディスク領域、物理ボリューム領域等の記憶領域と、記憶制御装置のポートと、アクセス可能な上位装置のN\_Port\_Name情報とを対応づけて管理する手段を有し、記憶領域毎に不正アクセスを抑止する手段を有することを特徴とするファイバチャンネル接続記憶制御装置。

【請求項4】請求項2記載のファイバチャンネル接続記憶制御装置において、

当該記憶制御装置配下の記憶装置が、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらのライブラリ装置のいずれかである場合に、当該記憶制御装置は、アクセス可能な上位装置、記憶制御装置のポート、記憶装置の対応付けを行い、ライブラリ装置の場合

はさらにドライブ、媒体の対応付けも行つて、テーブルで管理、保持する手段を有し、上位装置からの不正アクセスを防止する手段を有することを特徴とするファイバチャンネル接続記憶制御装置。

【請求項5】請求項1、2、3、4記載のファイバチャンネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、パネルを用いて設定可能であることを特徴とするファイバチャンネル接続記憶制御装置。

10 【請求項6】請求項1、2、3、4記載のファイバチャンネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、パネルを用いて設定可能であり、さらに、当該情報の設定時の保護策を具備していることを特徴とするファイバチャンネル接続記憶制御装置。

【請求項7】請求項1、2、3、4記載のファイバチャンネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、上位装置のユーティリティプログラムを用いて設定可能であることを特徴とするファイバチャンネル接続記憶制御装置。

【請求項8】請求項1、2、3、4記載のファイバチャンネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、上位装置のユーティリティプログラムを用いて設定可能であり、さらに、当該情報の設定時の入力保護策を具備していることを特徴とするファイバチャンネル接続記憶制御装置。

【請求項9】ネットワークアーキテクチャ形のチャンネルを、複数の上位装置と、記憶制御装置との間のインタフェースとし、上位装置、記憶制御装置、及び、記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、

上位装置を一意に識別できる上位装置識別情報を、複数の上位装置の立ち上がる以前に、記憶制御装置に設定しておき、上位装置が立ち上がり、上位装置識別情報を格納しているフレームを発行し、当該フレームを記憶制御装置が受領した際、記憶制御装置は、当該フレームに格納されている上位装置識別情報が当該記憶制御装置に既に設定されているかどうか、比較を行い、一致した場合は当該フレームの指示に基づく処理を継続し、不一致の場合は要求を拒絶することを特徴とするチャンネル接続記憶制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ANSIX3T11で標準化されたファイバチャンネルを上位装置とのインタフェースとする記憶制御装置に関し、特に上位装置、記憶制御装置及び当該記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、上位装置から当該

記憶制御装置に当該記憶装置へのアクセス要求があった際の、不正アクセス防止を行う記憶制御装置に関する。

【0002】

【従来の技術】ネットワーク上の不正アクセス防止に関しては、従来から種々の技術が知られている。

【0003】例えば、特開平3-152652号公報には、TCP/IPをサポートするコンピュータシステム間のネットワークセキュリティシステムとして、ログインできるユーザIDをメモリに定義しておくことにより、定義されたユーザID以外でログインしようとする

と、そのネットワークを切断する機能を持たせることが開示されている。

【0004】また、特開昭63-253450号公報には、中央処理装置のオペレーティングシステムがユーザID、パスワード、回線アドレスをチェックすることにより、ディスク装置のファイルへの不正アクセス防止を行なうことが示されている。

【0005】さらに、IBM社のESCONインタフェースでは、上位装置が当該上位装置の論理アドレスをソースアドレスとしてフレームに格納し、送信して

くことを利用して、記憶制御装置が事前に記憶制御装置に設定した論理アドレスとフレーム内の論理アドレスが一致するか否かをチェックする機能を設けている。

【0006】上述した従来技術は、上位論理層に1種類のレイヤを搭載するインタフェースを対象とした不正アクセス防止手段の域を出ないものである。

【0007】しかし、ANSIX3T11で標準化されたファイバチャネルは、ネットワーク形アーキテクチャであり、上位論理層にはTCP/IP、SCSI、ESCON、IPI等の種々のレイヤを搭載可能である。すなわち、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、他のインタフェースと論理的に互換性を持ち、物理的に自由にアクセス可能である。特に、このファイバチャネルと、ディスクアレイ装置等の複数の記憶領域を有する記憶装置とを備えた記憶システムにおいては、上記記憶領域は多くの上位装置に共用される。したがって、従来の不正アクセス防止策では不十分であり、ユーザが意識したセキュリティ設定により、機密保持を行なう必要がある。

【0008】

【発明が解決しようとする課題】本発明は、ANSIX3T11で標準化されたファイバチャネルを、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び、この記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、物理的にあらゆる上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを拒絶する手段を持たなかった記憶制御装置に対し、上位装置からの不正なアクセスを防止するセキュリティ機能を持つファイ

バチャネル接続記憶制御装置を提供することを目的とする。

【0009】さらに、本発明は、上位装置からの不正アクセス防止のために、アクセス可能な上位装置を容易に管理できる方式を持つファイバチャネル接続記憶制御装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明によれば、上記目的は、アクセス可能な上位装置の、上位装置を一意に識別するN\_\_Port\_\_Name情報を当該記憶制御装置に設定し、上位装置から送られてくるフレーム内に格納されたN\_\_Port\_\_Name情報と比較し、アクセスの可否を決定することにより達成される。

【0011】上記目的を達成するための本発明の具体的な特徴は、上位装置から発行される、上位装置を一意に識別する情報であるN\_\_Port\_\_Name情報を、パネル等を用いて入力し、入力情報を記憶制御装置の制御メモリに、制御テーブルとして格納する手段を有することである。この際、記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有することが望ましい。

【0012】そして、上記制御テーブルを不揮発制御メモリに格納するようにすれば、万一の電源瞬断時にも管理情報を守ることができる。

【0013】さらに、本発明の具体的な特徴によれば、上位装置が立ち上がった後、上位装置がN\_\_Port\_\_Name情報を格納したフレームを記憶制御装置に対し発行し、記憶制御装置がこれを受領した際、記憶制御装置は既に設置され、保持されている上位装置を一意に識別するN\_\_Port\_\_Name情報と、受領したフレームに格納されたN\_\_Port\_\_Name情報とを比較する手段を有し、比較により一致した場合は、記憶制御装置は当該フレームの指示に基づく処理を継続し、不一致の場合は、受領した当該フレームを拒絶するLS\_\_RJ Tフレームを上位装置に返すようにしたことである。これにより、記憶制御装置は上位装置からの不正アクセスを抑止することができる。

【0014】さらに、本発明の具体的な特徴によれば、当該記憶制御装置が有する上位インタフェース（ポート）の物理的な数以上のN\_\_Port\_\_Name情報を設定する手段を有することである。すなわち、1ポートで複数のN\_\_Port\_\_Name情報を設定する手段を有することである。これにより、ファイバチャネルファブリック（Fabric）またはスイッチ接続時の論理パス多重構成に対応できる。

【0015】また、当該記憶制御装置の配下に、ディスクアレイ装置のような、多くの磁気ディスクボリュームを有し、複数のチャネルパスルートを有すシステムにおいては、チャネルパスルート毎に、当該記憶制御装置配下のLUN（ロジカルユニットナンバ）による論理ディ

スク領域、物理ボリューム領域、RAIDグループによる論理ディスク領域等の記憶領域と、記憶制御装置のポート、上位装置のN\_Port\_Name情報との対応付けを記憶制御装置内で管理する手段を有することである。これにより、ユーザは、記憶領域毎に、不正アクセスを防止することができ、木目細かいアクセス管理が可能となる。

【0016】さらに、本発明においては、記憶制御装置配下の記憶装置が磁気ディスク装置、ディスクアレイ装置の代わりに、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらの各種ライブラリ装置の何れの場合でも、当該記憶制御装置は、アクセス可能な上位装置のN\_Port\_Name情報、記憶制御装置のポート、記憶装置の対応付けを行い、ライブラリ装置の場合はさらにドライブ、媒体の対応付けも行つて、制御テーブルで管理、保持する手段を有し、フレーム受領の際にフレーム内の情報と制御テーブル内の情報を比較する手段を有し、上位装置からの不正アクセスの防止を行うことができる。

【0017】さらに、本発明では、記憶制御装置が管理する情報を、パネル等を用いて設定する際、パスワードを入力する等により、管理情報を保護する手段を具備する。これにより、ユーザは当該情報の不正な登録、不正な再設定を防止することができる。また、ユーザは管理情報の設定を行うだけで、容易に不正アクセスを防止可能であり、ユーザの負担が少ない。

【0018】なお、本発明において、記憶制御装置が管理する情報を設定する手段として、上述のように、パネル等を用いて設定する他に、上位装置のユーティリティプログラムを用いて設定することも可能である。

#### 【0019】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。まず、図1ないし図5を用いて、本発明の対象となるファイバチャネル及びそれを用いて構成した記憶システムについて説明する。

【0020】図1は、記憶制御装置配下の記憶装置がディスクアレイ装置の場合の記憶システムのハードウェア構成図である。図1において、10、20、30は、データ処理を行う中央処理装置としての上位装置である。

【0021】40は、本発明を実施したディスクアレイ装置の記憶制御装置である。図1に示すように、記憶制御装置40は、上位装置10、20、30との間のデータ転送を制御するためのDMA（ダイレクト アクセス メモリ）を含むプロトコルプロセッサであるファイバチャネル制御部41、記憶制御装置全体を制御するマイクロプロセッサ42、制御装置の動作を制御するマイクロプログラム及び制御用データを保存する制御メモリ43、キャッシュへのデータの読み書きを制御するキャッシュ制御部44、書き込みデータ及びディスクドライブからの読み出しデータを一時バッファリングしておくデ

ィスクキャッシュ45、ディスクドライブとの間のデータ転送を制御するためのDMAを含むプロトコルプロセッサであるデバイスインタフェース制御部46、装置構成情報を記憶制御装置へ入力するパネル47から構成されている。

【0022】50は、記憶制御装置40の配下にあるディスクアレイ装置である。ディスクアレイ装置50は、上位装置のデータを格納する装置で、複数台の個別ディスクを冗長性を持つように配置構成したものである。

【0023】ディスクアレイ装置50を構成するディスクは、論理的に分割し、分割した区画をそれぞれ異なるRAIDレベルに設定することができる。この区画をRAIDグループという。このRAIDグループをさらに論理的に分割したSCSIのアクセス単位である領域をLU（Logical Unit）といい、その領域は、各々、LUN（Logical Unit Number）という番号を持つ。本実施の形態ではディスクアレイ装置50は、LUN0番のLUである、LU0（51）とLUN1番のLUである、LU1（52）の2個の領域を有する場合を示している。

【0024】なお、LUの数は、図1に示す2個に限らずもっと多くてもよく、シングルターゲット機能の場合、ターゲット当たり最大8個までLUを設定できる。

【0025】また、本実施の形態では、LUなる記憶領域をアクセス単位としているが、アクセス単位とする記憶領域としては、物理ボリューム単位やRAIDグループ単位の記憶領域も可能である。

【0026】上位装置10、20、30と記憶制御装置40は、ファイバチャネル60をインタフェースとし、ファブリック（Fabric）という装置を介して接続されている。

【0027】図1のシステムの動作を、上位装置10が記憶制御装置40経由でディスクアレイ装置50とデータ転送を行う場合を例にとり、制御の流れ、データの流れを中心に説明する。

【0028】上位装置10がアクセス要求を出すと、その要求を認識したファイバチャネル制御部41はマイクロプロセッサ42に割り込み要求を発行する。マイクロプロセッサ42は、上位装置からのコマンド情報及び本発明で必要な制御情報を、制御メモリ43に格納する。

【0029】コマンド情報が、ライトコマンドの場合は、マイクロプロセッサ42はファイバチャネル制御部41にデータ転送を指示し、転送されたデータをキャッシュ制御部44を経由してキャッシュ45に格納する。上位装置10に対しては、ファイバチャネル制御部41がライト完了報告を行う。ライト完了報告後、マイクロプロセッサ42がデバイスインタフェース制御部46を制御し、ディスクアレイ装置50に対し、データ及び冗長データを書き込む。この場合、一般のRAID5の動作においては、旧データ、旧パリティ及び新データに基

いて新パリティを作成するが、本発明の制御によれば、マイクロプロセッサ42が、デバイスインタフェース制御部46及びキャッシュ制御部44、制御メモリ43、キャッシュ45を用いて行なう。

【0030】一方、上位装置10からコマンド情報として、リードコマンド情報を受けた場合は、マイクロプロセッサ42は、デバイスインタフェース制御部46に指示を出し、当該アクセス要求のデータブロックが格納されたディスクアレイ装置50へアクセスしてデータを読み出し、キャッシュ制御部44を経由してキャッシュ45へデータを格納する。マイクロプロセッサ42は、ファイバチャネル制御部41に指示を出し、ファイバチャネル制御部41は、キャッシュ45に格納したデータを上位装置10に転送し、転送後上位装置へリード完了報告を行なう。

【0031】次にファイバチャネル60の特長を説明する。ファイバチャネルは最大10kmの距離で100MB/sの転送が可能な高速インタフェースである。ファイバチャネルのアーキテクチャは転送元のバッファから転送先のバッファへデータを送るが、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、異なるネットワーク通信プロトコルを処理するオーバーヘッドがなく、高速データ転送を実現している。上位論理層にはTCP/IP、SCSI、ESCON、IPI等の種々のレイヤを搭載可能である。すなわち、他のインタフェースと論理的に互換性を持つ。複雑な装置間の接続/交換という機能はFabricと呼ぶ装置が行ない、論理パス多重構成を組むことが可能である。

【0032】ファイバチャネルがデータをやりとりする基本単位をフレームと言う。次に、このフレームについて、図2を用いて説明する。

【0033】図2に示すように、フレーム70は、スタートオブフレームSOF(Start Of Frame)71、フレームヘッダ72、データフィールド73、サイクリックリダンダンシチェックCRC(Cyclic Redundancy Check)74及びエンドオブフレームEOF(End Of Frame)75で構成される。

【0034】SOF71は、フレームの先頭に置く4バイトの識別子である。

【0035】EOF75は、フレームの最後につける4バイトの識別子で、SOF71とEOF75によりフレームの境界を示す。ファイバチャネルではフレームがない時はアイドル(idle)という信号が流れている。

【0036】フレームヘッダ72は、フレームタイプ、上位プロトコルタイプ、送信元と送信先のN\_Port\_ID情報、N\_Port\_Name情報等を含む。N\_Port\_IDはアドレスを表わし、N\_Port\_Nameはポートの識別子を表わす情報である。

【0037】データフィールド73の先頭部には上位レイヤのヘッダを置くことができる。これにデータそのものを運ぶペイロード部が続く。CRC74は、フレームヘッダとデータフィールドのデータをチェックするための、4バイトのチェックコードである。

【0038】上記フレームヘッダ72のフォーマット80を、図3に示す。フレームヘッダフォーマット80において、デスティネーションアイデンティファイアD\_ID(Destination ID)81はフレーム受け取り側のアドレス識別子であり、また、ソースアイデンティファイアS\_ID(Source ID)82はフレーム送信側のN\_Portアドレス識別子であり、各々、N\_Port\_ID、N\_Port\_Name情報等を含む。

【0039】次に図4を用いて、フレームを構成するデータフィールド73のペイロードの1つである、ファイバチャネルプロトコルコマンドFCP\_CMND(Fibre Channel Protocol for SCSI Command)のペイロード90の説明を行なう。

【0040】FCPロジカルユニットナンバFCP\_LUN(FCP Logical Unit Number)フィールド91には、コマンドを発行するロジカルユニット番号LUNが指定される。FCPコントロールFCP\_CNTL(FCP Control)フィールド92には、コマンド制御パラメータが指定される。そして、FCPコマンドデスクリプタブロックFCP\_CDB(FCP Command Descriptor Block)フィールド93には、SCSIコマンドデスクリプタブロック(SCSI Command Descriptor Block)が格納され、リードコマンドRead等のコマンド種類、LUN等のアドレス、ブロック数が示される。FCPデータレングスFCP\_DL(FCP Data Length)フィールド94には、当該コマンドにより転送されるデータ量がバイト数で指定される。

【0041】以上のように構成されたフレームによってデータのやりとりが行われる。

【0042】フレームは機能に基づいてデータフレームとリンク制御フレームとに大別される。データフレームは、情報を転送するために用い、データフィールドのペイロード部に上位プロトコルで使用するデータ、コマンドを搭載する。

【0043】一方、リンク制御フレームは、一般に、フレーム配信の成功あるいは不成功を示すのに使われる。フレームを1個受領したことを示したり、ログインする場合に転送に関するパラメータを通知したりするフレーム等がある。

【0044】次に、図5を用いて、「シーケンス」について説明する。ファイバチャネルにおけるシーケンス

は、あるN\_\_Portから別のN\_\_Portへ、一方向に転送される関連するデータフレームの集まりのことを言い、SCSIのフェーズに相当する。シーケンスの集まりをエクスチェンジと呼ぶ。例えばコマンドを発行して、そのコマンドの終了までに、そのコマンド実行のためにやりとりされるシーケンスの集まり（コマンド発行、データ転送、終了報告）がエクスチェンジとなる。このように、エクスチェンジはSCSIのI/Oに相当する。

【0045】図5（a）、（b）及び（c）は、それぞれ、ログインシーケンス（100）、リードコマンドシーケンス（110）及びライトコマンドシーケンス（120）を示す。

【0046】ファイバチャネルインタフェースでは、上位装置がデバイスに対し、通信パラメータを含むポートログインPLOGI（N\_\_Port Login）フレームを送り、デバイスがこれを受け付けることで通信が可能となる。これをログインと呼ぶ。図5（a）に、ログインシーケンス（100）を示す。

【0047】図5（a）のログインシーケンス（100）において、まず、シーケンス101で、上位装置はデバイスに対し、PLOGIフレームを送り、ログインの要求を行なう。デバイスはアクノレッジACK（Acknowledge）フレームを上位装置に送り、PLOGIフレームを受け取ったことを知らせる。

【0048】次いで、シーケンス102において、デバイスは、ログイン要求を受け付ける場合はアクセプトACC（Accept）フレームを、要求を拒絶する場合はリンクサービスリジェクトLS-RJT（Link Service Reject）フレームを、それぞれ、上位装置に送る。

【0049】次に、図5（b）のリードコマンドのシーケンス（110）を説明する。

【0050】シーケンス111において、上位装置はデバイスに対し、FCP\_\_CMNDフレームを送り、リード要求を行なう。デバイスはACKフレームを上位装置に送る。

【0051】シーケンス102では、デバイスは、FCPトランスファレディFCP\_\_XFER\_\_RDY（FCP Transfer Ready）フレームを上位装置に送り、データ転送の準備ができたことを知らせる。上位装置はACKフレームをデバイスに送る。

【0052】シーケンス113に進み、デバイスはFCPデータ（FCP\_\_DATA）フレームを上位装置に送り、データを転送する。上位装置はACKフレームをデバイスに送る。

【0053】次のシーケンス114では、デバイスはFCP\_\_RSPフレームを上位装置に送り、データの転送が正常終了したことを知らせる。上位装置はACKフレームをデバイスに送る。

【0054】次に、図5（c）のライトコマンドのシーケンス（120）を説明する。

【0055】シーケンス121において、上位装置はデバイスに対し、FCP\_\_CMNDフレームを送り、ライト要求を行なう。デバイスはACKフレームを上位装置に送る。

【0056】次いで、シーケンス122において、デバイスはFCP\_\_XFER\_\_RDYフレームを上位装置に送り、データ書き込みが可能であることを知らせる。上位装置はACKフレームをデバイスに送る。

【0057】さらに、シーケンス123において、上位装置はFCP\_\_DATAフレームをデバイスに送り、データを転送する。デバイスはACKフレームを上位装置に送る。

【0058】最後に、シーケンス123において、デバイスは、FCPレスポンスFCP\_\_RSP（FCP Response）フレームを上位装置に送り、データの受け取りが正常終了したことを知らせる。上位装置はACKフレームをデバイスに送る。

【0059】以上、図1ないし図5によって、一般的なシステム構成、フォーマット及びシーケンスを説明したが、以下、本発明によるセキュリティチェックについて説明する。

【0060】初めに、PLOGI時におけるN\_\_Port\_\_Name情報を用いたセキュリティチェックについて、説明を行なう。

【0061】本発明では、図1において、まず、上位装置10、20、30の立ち上がる以前に、ユーザは記憶制御装置40のマイクロプロセッサ42にアクセス可能な上位装置のリストを設定する。すなわち、上位装置を識別できるN\_\_Port\_\_Name、N\_\_Port\_\_ID等の情報を、パネル47を用いて入力する。この際、パネルへの入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化できる。

【0062】パスワードを入力し、既に設定したパスワードとの一致が図られた場合、記憶制御装置のポート毎にアクセス可能な上位装置のN\_\_Port\_\_Name情報を入力し、入力情報を制御テーブルに格納する。

【0063】いま、例として、上位装置10、20はディスクアレイ装置50にアクセス可能、上位装置30はディスクアレイ装置50にはアクセス不可能とし、N\_\_Port\_\_Nameを、上位装置10はHOSTA、上位装置20はHOSTB、上位装置30はHOSTCとし、記憶制御装置40のファイバチャネル制御部41のポートをCTLOP0とした場合、ログイン要求制御テーブル130は、図6のようになる。

【0064】図6に示すこのログイン要求制御テーブル130を、不揮発メモリ上に設定することにより、万一の電源瞬断時にも管理情報を守ることができる。

【0065】また、ログイン要求制御テーブル130に格納した情報は、電源を切断した場合はハードディスク領域50へ格納する。または情報の更新時にメモリ43とディスク50へ反映を行なう。これにより記憶制御装置40は、当該情報を再設定されるまで恒久的に保持することができる。

【0066】なお、ファイバチャネルにおいてノードやポートの識別に使用される自ノード情報として、N\_\_Port\_\_Nameの他に、N\_\_Port\_\_IDがあるが、N\_\_Port\_\_IDは変更される可能性があり、ユーザが管理する数値ではないため、N\_\_Port\_\_Name情報をセキュリティのためのチェック対象とすることが望ましい。

【0067】次に、図1及び図7を用いて上位装置のログイン要求に対する記憶制御装置のフレーム処理手順の説明を行なう。

【0068】(ステップS71) 上位装置10、20、30が立ち上がり、各々、N\_\_Port\_\_Name情報を格納したログイン要求フレームであるPLOGIフレームを発行する。記憶制御装置40のマイクロプロセッサ42は、当該フレームを受領すると、まずこのフレームを受領したことを示すACKフレームを各上位装置に返す。

【0069】(ステップS72) そしてマイクロプロセッサ42は、当該フレームに格納されているN\_\_Port\_\_Name情報を切り出し、そのN\_\_Port\_\_Name情報が、既に設定され、保持されている制御テーブル内のN\_\_Port\_\_Nameリストに登録されているかどうか、比較を行なう。

【0070】(ステップS73) (ステップS74) (ステップS75)

上位装置10、20の発行した当該フレームに格納されているN\_\_Port\_\_Name情報は、制御テーブル内に登録されているN\_\_Port\_\_Name情報と一致するため、記憶制御装置40のマイクロプロセッサ42は、上位装置10、20に対してはログイン要求を受け付けた印として、ACCフレームを返し、ログイン処理を続行する。

【0071】(ステップS73) (ステップS76)

一方、上位装置30の発行した当該フレームに格納されているN\_\_Port\_\_Name情報は、制御テーブル内に登録されているN\_\_Port\_\_Name情報と一致しないため、記憶制御装置40のマイクロプロセッサ42は、上位装置30に対しては接続を拒絶するリジェクトパラメータをいれたLS\_RJTフレームを返す。

【0072】以上のように、記憶制御装置40が、ログイン要求制御テーブル130を用いて、上位装置と記憶制御装置のポートの対応付けを管理することにより、ユーザはポート毎に上位装置からの不正アクセスを抑止することができ、セキュリティが保持できる。

【0073】次に、本発明において、ディスクアレイ装置の記憶領域であるLUN毎に、N\_\_Port\_\_Name情報を用いてセキュリティチェックを実施する方法について説明する。

【0074】本発明では、まず上位装置10、20、30の立ち上がる以前に、記憶制御装置40のマイクロプロセッサ42に、LUN毎にアクセス可能な上位装置のリストを設定する。上位装置を識別できるN\_\_Port\_\_Name、N\_\_Port\_\_ID等の情報を、パネル47を用いて入力する。この際、パネル47への入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化することができる。

【0075】パスワードを入力し、既に設定したパスワードとの一致が図られた場合、LUN毎に記憶制御装置のポート及びアクセス可能な上位装置のN\_\_Port\_\_Name情報を入力し、入力情報を制御テーブルに格納する。

【0076】LU0(51)は、上位装置10から記憶制御装置40のファイバチャネル制御部41のポート経由でアクセス可能、LU1(52)は、上位装置20から記憶制御装置40のファイバチャネル制御部41のポート経由でアクセス可能とし、N\_\_Port\_\_Nameを、上位装置10はHOSTA、上位装置20はHOSTB、記憶制御装置40のファイバチャネル制御部41のポートをCTLOP0、とした場合、I/O要求制御テーブル140は、図8のようになる。

【0077】図8に示すこのI/O要求制御テーブル140は不揮発メモリ上に設定すると、万一の電源瞬断時にも管理情報を守ることができる。

【0078】また、図8のI/O要求制御テーブル140に格納した情報は、電源を切断した場合は、ハードディスク領域50へ格納する。または情報の更新時にメモリ43とディスク50へ反映を行なう。これにより記憶制御装置40は当該情報を再設定されるまで恒久的に保持することができる。

【0079】本実施例ではチャネルパスルートは1通りであるが、複数のチャネルパスルートを有するシステムにおいても同様である。

【0080】以下に図1及び図9を用いて、上位装置のI/O要求に対する記憶制御装置のフレーム処理手順の説明を行なう。上記の例ではPLOI時にセキュリティチェックを行なったが、本実施の形態では、各SCSIコマンド毎にチェックを行なう。

【0081】(ステップS91) 上位装置10がLU0(51)にI/O要求を出したい場合、上位装置10は記憶制御装置40に対し、SCSI CDBを格納したフレームを発行する。記憶制御装置40がこのフレームを受領した場合、まず、このフレームを受領したことを示すACKフレームを上位装置10に返す。

【0082】(ステップS92) そしてマイクロプロセ

ッサ42は、当該フレームに格納されているN\_\_Port\_\_Name情報及びCDB内のLUN番号を切り出し、そのN\_\_Port\_\_Name情報及びLUN番号が、当該マイクロプロセッサ42に既に設定され保持されている制御テーブル内のリストに登録されているかどうか、比較を行なう。

【0083】(ステップS93)(ステップS94)(ステップS95)

管理テーブル内には、「上位装置10は、LU0(51)をアクセス可能である」と登録されているため、記憶制御装置40のマイクロプロセッサ42はコマンドを受領し、I/O処理を継続する。

【0084】(ステップS91)一方、上位装置20が記憶制御装置40にLU0(51)のI/O要求フレームを発行し、記憶制御装置40がこのSCSI CDBを格納したフレームを受領した場合、マイクロプロセッサ42は、まずこのフレームを受領したことを示すACKフレームを上位装置20に返す。

【0085】(ステップS92)そしてマイクロプロセッサ42は、当該フレームに格納されているN\_\_Port\_\_Name情報及びCDB内のLUN番号を切り出し、そのN\_\_Port\_\_Name情報及びLUN番号が、管理テーブル内にあるかどうかの検索を行なう。

【0086】(ステップS93)(ステップS96)検索を行なった結果、管理テーブル内に、該当するLUNおよびN\_\_Port\_\_Nameの組み合わせが存在しないため、記憶制御装置40のマイクロプロセッサ42は、上位装置20にLS\_\_RJTフレームを送って、I/O要求を拒絶する。

【0087】こうして記憶制御装置は不正なアクセスを防止することができる。

【0088】ここではログイン及びI/O要求フレームを取り上げたが、これら以外の他の上位装置フレームに格納されているN\_\_Port\_\_Name情報を比較してもよい。

【0089】なお、ファイバチャネル接続記憶制御装置配下の記憶装置がディスクアレイ装置に限らず、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらのライブラリ装置である場合にも本発明を適用できる。

【0090】記憶制御装置配下の記憶装置が光ディスクライブラリ装置の場合に本発明を適用した場合の概要を図10を用いて説明する。150は記憶制御装置40配下の光ディスクライブラリ装置であり、151は光ディスクドライブ、152から156は光ディスクの媒体である。

【0091】ユーザは上位装置10、20、30が立ち上る前にパネルを使用して、媒体、ドライブ、ポートとN\_\_Port\_\_Name情報との対応付けを設定し、上位装置のアクセス権限をマイクロプログラムに保持して

おく。

【0092】媒体152、153、154は、上位装置10からアクセス可能、媒体D155、E156は上位装置20からアクセス可能とし、N\_\_Port\_\_Nameを上位装置10はHOSTA、上位装置20はHOSTB、記憶制御装置40のポートをCTLOP0、光ディスクドライブA151をDRIVE0、媒体A152、B153、C154、D155、E156を各々MEDA、MEDB、MEDC、MEDD、MEDE、とした場合、要求制御テーブル160は、図11のようになる。

【0093】各上位装置がI/O要求フレームを発行した際、フレームを構成するペイロード内のCDBにボリューム情報が格納されているため、記憶制御装置40は当該フレームを受領した際、フレーム内のN\_\_Port\_\_Name情報及びペイロード内の媒体識別子を、当該記憶制御装置40に既に設定され、保持されている制御テーブルと比較を行なえばよい。このように、本発明を応用することによって、記憶制御装置は上位装置からの不正アクセスを防止可能である。

【0094】

【発明の効果】以上述べたように、本発明によって、ANSIX3T11で標準化されたファイバチャネルを上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、不正な上位装置からのアクセスを抑止することができるので、記憶装置内のデータの機密保護を行うことができる。

【0095】また、上位装置、記憶制御装置のポート、記憶領域を対応付けて上位装置からのアクセスを木目細かに管理できるので、記憶領域毎に用途を変える等、記憶装置をニーズに合わせて活用することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すハードウェア構成図である。

【図2】第1の実施の形態におけるフレームのフォーマット図である。

【図3】図2で示したフレームを構成するフレームヘッダのフォーマット図である。

【図4】図2で示したフレームの一つであるFCP\_\_CMNDのペイロードのフォーマット図(a)及び当該ペイロードを構成するFCP\_\_CDBのフォーマット図(b)である。

【図5】第1の実施の形態において上位装置とデバイスがデータフレームのやりとりを行なうシーケンスの例を示し、ログイン時のシーケンス図(a)、リードコマンド時のシーケンス図(b)及びライトコマンド時のシーケンス図(c)である。

【図6】第1の実施の形態において、記憶制御装置が、上位装置を管理する制御テーブルを示した図である。



【図7】第1の実施の形態において、記憶制御装置が、上位装置（ホスト）からのログイン要求時に実行するフレーム処理のフローチャートである。

【図8】第1の実施の形態において、記憶制御装置が、記憶領域を管理する制御テーブルを示した図である。

【図9】第1の実施の形態において、記憶制御装置が、ホストからのI/O要求時に実行するフレーム処理のフローチャートである。

【図10】本発明の第2の実施の形態として、記憶制御装置配下の記憶装置が、光ディスクライブラリの場合を示すハードウェア構成図である。

【図11】図10に示す第2の実施の形態において、記憶制御装置が管理する制御テーブルを示した図である。

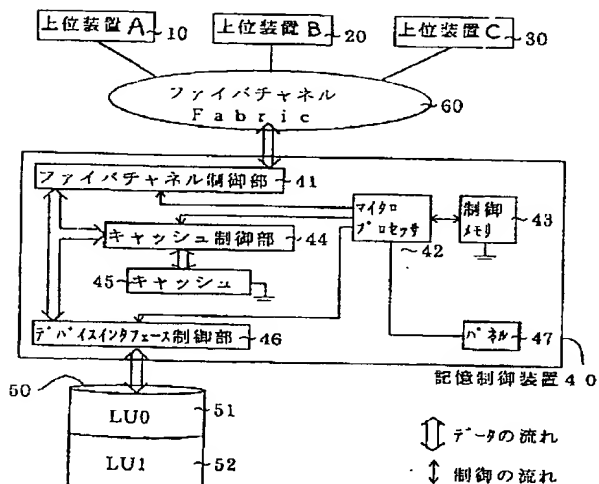
#### 【符号の説明】

10、20、30…上位装置、40…記憶制御装置、41…ファイバチャネル制御部、42…マイクロプロセッサ、43…制御メモリ、44…キャッシュ制御部、45…キャッシュ、46…デバイスインタフェース制御部、47…パネル、50…ディスクアレイ装置、51…ロジカルユニット0、52…ロジカルユニット1、60…ファイバチャネル、70…フレーム、71…スタートオブフレームSOF (Start Of Frame)、72…フレームヘッダ、73…データフィールド、74…サイクリックリダンダンシチェックCRC (Cycli

cRedundancy Check)、75…エンドオブフレームEOF (End Of Frame)、80…フレームヘッダのフォーマット、81…デスティネーションアイデンティファイアD\_ID (Destination ID)、82…ソースアイデンティファイアS\_ID (Source ID)、90…ファイバチャネルプロトコルコマンドFCP\_CMNDペイロード (Fibre Channel Protocol for SCSI Command)、91…ファイバチャネルプロトコルロジカルユニットナンバFCP\_LUN (FCP Logical Unit Number)、92…ファイバチャネルプロトコルコントロールFCP\_CNTL (FCP Control)、93…ファイバチャネルプロトコルコマンドデスク립タブロックFCP\_CDB (FCP Command Descriptor Block)、94…ファイバチャネルプロトコルデータレングスFCP\_DL (FCP Data Length)、100…ログイン、110…リードコマンド、120…ライトコマンド、130…ログイン要求制御テーブル、140…磁気ディスクアレイI/O要求制御テーブル、150…光ディスクライブラリ、160…光ディスクライブラリI/O要求制御テーブル

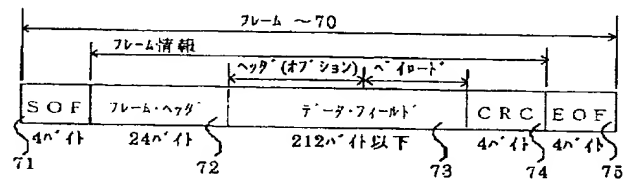
【図1】

図1



【図2】

図2



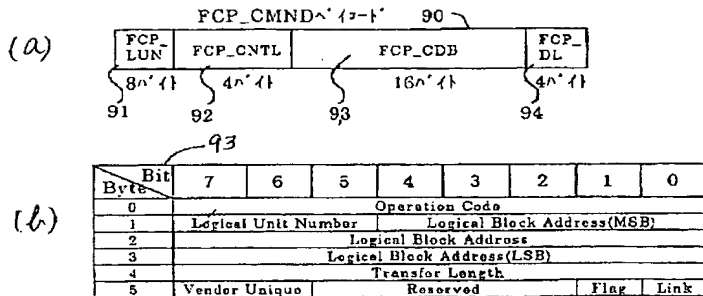
【図3】

図3

Bit	31-24	23-16	15-8	7-0
0	R_CTL	D_ID(フレーム受け取り側の N_Portアドレス識別子)		
1	Reserved	S_ID(フレーム送信側の N_Portアドレス識別子)		
2	TYPE		F_CTL	
3	SEQ_ID	DF_CTL	SEQ_CNT	
4		OX_ID		RX_ID
5	Parameter			

【図4】

図4



【図6】

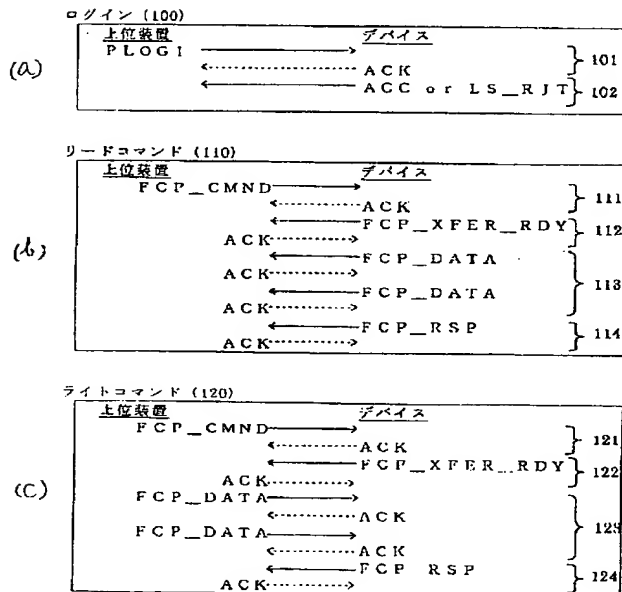
図6

制御テーブル 130

上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
HOSTA	CTL0P0
HOSTB	CTL0P0

【図5】

図5



【図8】

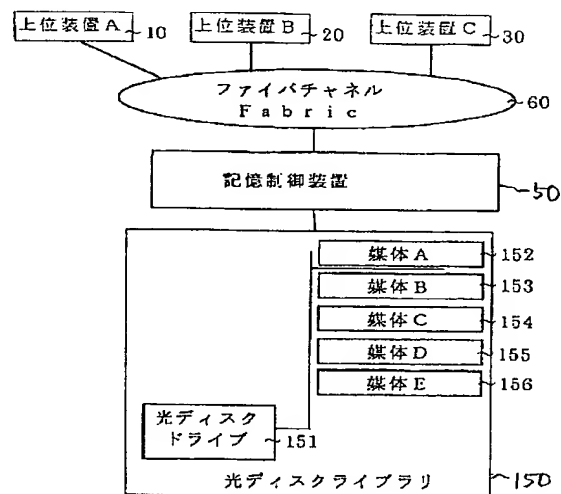
図8

制御テーブル 140

記憶領域 LU	上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
LU0	HOSTA	CTL0P0
LU1	HOSTB	CTL0P0

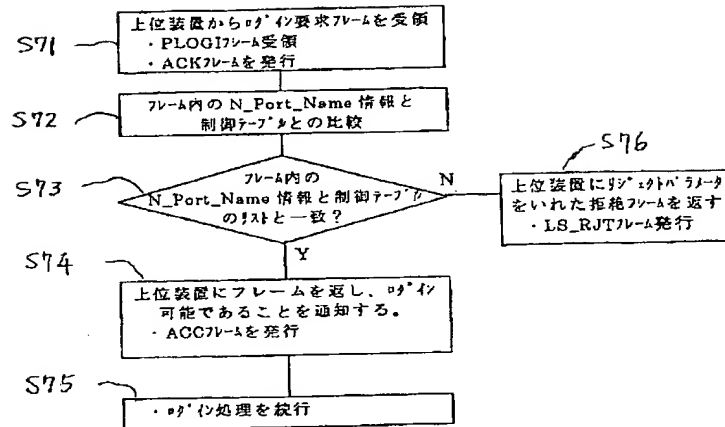
【図10】

図10



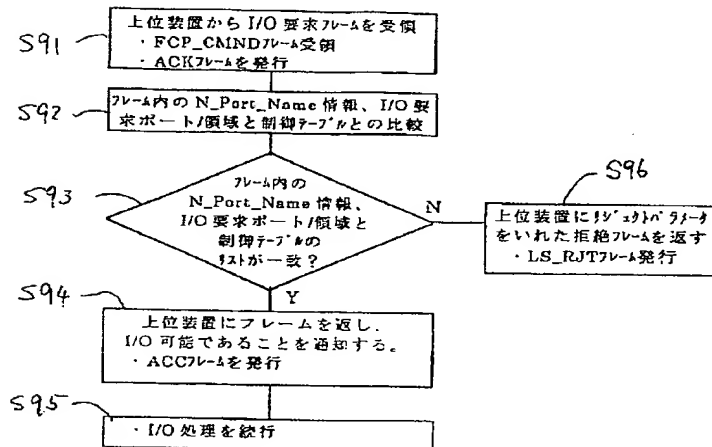
【図7】

図7



【図9】

図9



【図11】

図11

制御テーブル 160

記憶領域 光ディスク媒体	光ディスク ドライブ	上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
MEDA	DRIVE0	HOSTA	CTL0P0
MEDB	DRIVE0	HOSTA	CTL0P0
MEDC	DRIVE0	HOSTA	CTL0P0
MEDD	DRIVE0	HOSTB	CTL0P0
MEDE	DRIVE0	HOSTB	CTL0P0

## フロントページの続き

(72)発明者 佐藤 雅彦  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内  
(72)発明者 村岡 健司  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内

(72)発明者 高木 賢一  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内  
(72)発明者 小林 正明  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内

(19) 日本国特許庁(JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2000-276406

(P 2000-276406 A)

(43) 公開日 平成12年10月6日(2000.10.6)

(51) Int. Cl. 7	識別記号	F I	テーマコード(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	A 5B017
3/06	3 0 1	3/06	A 5B065

審査請求 未請求 請求項の数 5

O L

(全 1 4 頁)

(21) 出願番号 特願平11-85393

(22) 出願日 平成11年3月29日(1999. 3. 29)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 小笠原 裕

神奈川県小田原市国府津2880番地 株式会

社日立製作所ストレージシステム事業部内

(72) 発明者 岡見 吉規

神奈川県小田原市国府津2880番地 株式会

社日立製作所ストレージシステム事業部内

(74) 代理人 100068504

弁理士 小川 勝男

F ターム(参考) 5B017 AA01 BA01 BB03 BB06 CA09

CA16

5B065 CA01 CC01 PA02 PA04 PA13

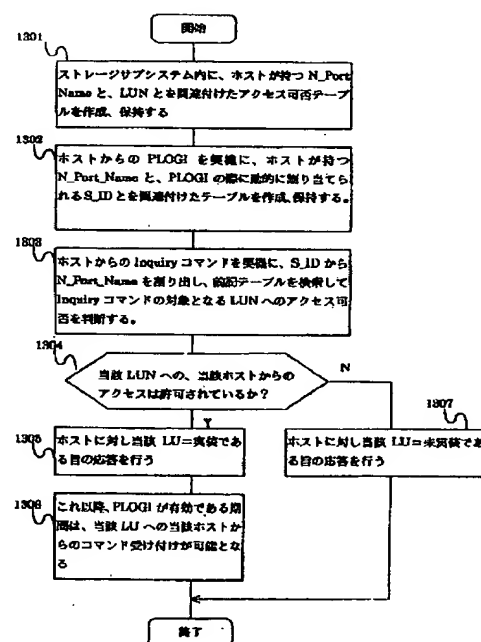
(54) 【発明の名称】 ファイバチャネル接続ストレージサブシステム及びそのアクセス方法

(57) 【要約】

【課題】 ホストからストレージサブシステム内の記憶領域(LU)へのアクセスを選択的に制限することにより、不正アクセスを防止する。またこの際、アクセスの可否を判定する際生じるオーバーヘッドが最小限となる方法を提供し、かつ判定の条件を標準ファイバチャネルプロトコルの範囲のみで行える方法を提供する。

【解決手段】 ホストのN\_Port\_Name或いはNode\_Nameとストレージサブシステム内のLUを関連付けるアクセス可否テーブル(1301)と、ホストがログインする際に割り当てるS\_IDとLUとを関連付ける関連テーブル(1302)とを作成・保持し、ホストからのInquiry要求のS\_IDと前記両テーブルとを用いてLUへのアクセス可否を判断し(1303)、ホストへ通知する(1304)。

図 13



## 【特許請求の範囲】

【請求項 1】情報を記憶するドライブデバイスと、このドライブデバイスに情報を書き込み或いはこのドライブデバイスからの情報の読み込みを制御するデバイスドライバ制御部と、上位装置からのコマンドを受信するファイバチャネルインタフェースを持つポートと、前記コマンドに基づき前記デバイスドライバ制御部を制御して処理を行う演算装置とを備えたストレージサブシステムにおいて、

前記上位装置或いは上位装置のポートを識別する識別手段と前記ドライブデバイス内の特定の記憶領域とを関連付け前記上位装置から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルを設定するアクセス可否テーブル設定手段と、このアクセス可否テーブルを保持する保持手段とを備え、

前記演算装置は、前記上位装置からストレージサブシステムへの通信要求を受け付けた際にこの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを設定し、この関連テーブルとドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子とから前記識別手段を割り出し、この識別手段と前記アクセス可否テーブルとから上位装置のアクセス可否を判断するストレージサブシステム。

【請求項 2】前記演算装置は上位装置のアクセスを否と判断した場合には記憶領域が実装されていないという情報を上位装置に送信する請求項 1 に記載のストレージサブシステム。

【請求項 3】情報を記憶するドライブデバイスと、このドライブデバイスに情報を書き込み或いはこのドライブデバイスからの情報の読み込みを制御するデバイスドライバ制御部と、上位装置からのコマンドを受信するファイバチャネルインタフェースを持つポートと、前記コマンドに基づき前記デバイスドライバ制御部を制御して処理を行う演算装置とを備えたストレージサブシステムにおいて、

前記上位装置からストレージサブシステムへの通信要求を受け付けた際にこの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを設定する関連テーブル設定手段と、この関連テーブル及び前記上位装置或いは前記上位装置のポートを識別する識別手段と前記ドライブデバイス内の特定の記憶領域とを関連付け前記上位装置から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルとを保持する保持手段と、ドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子と前記関連テーブルとから割り出した前記識別子と前記アクセス可否テーブルとから上位装置のアクセス可否を判断する判断手段とを備えたストレージサブシステム。

【請求項 4】前記アクセス可否テーブルは前記ポート毎に作成する請求項 1 乃至 3 の何れか 1 項に記載のストレージサブシステム。

【請求項 5】前記上位装置或いは上位装置のポートを識別する識別手段とドライブデバイス内の特定の記憶領域とを関連付けこの記憶領域に対する上位装置のアクセス可否テーブルを作成・保持し、

前記上位装置からストレージサブシステムへの通信要求を受け付けた際に前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを作成・保持し、

この関連テーブルを用いてドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子から前記識別手段を割り出し、

割り出した識別手段と前記アクセス可否テーブルとを比較して前記上位装置のアクセス可否を判断するストレージサブシステムのアクセス方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、ANSI X3T11で標準化されたファイバチャネルプロトコルを、上位装置とのインタフェースとして持つストレージサブシステム（ディスクサブシステム）に係り、複数の上位装置からストレージサブシステム及びストレージサブシステム内の記憶領域へのアクセスを選択的に制限することにより、不正アクセスを防止できるストレージサブシステムに関する。

## 【0002】

【従来の技術】ANSI X3T11で標準化されたファイバチャネルプロトコルでは、多数の装置が接続可能であり、かつ SCSI、ESCON、TCP/IP 等多種のプロトコルを同時に運用可能な利点があるが、それに伴いセキュリティの確保が困難となる性質も併せ持っている。

【0003】ストレージサブシステムに対する不正アクセスを防止する方法としては、例えば特開平10-333839号公報では、ファイバチャネルプロトコルを用いた方法が開示されている。

【0004】この方法は、装置のインタフェース（ポートと呼ぶ）を、静的に一意に識別できる N\_Port\_Name について、上位装置を起動する前に予めストレージサブシステム中に記憶させ、かつこの N\_Port\_Name と、ストレージサブシステム中の特定ポート、或いは N\_Port\_Name とストレージサブシステム内部の任意の記憶領域とを関連付けるテーブルを保持し、上位装置起動後は、この上位装置がストレージサブシステムにアクセスする際に発行するフレームという情報単位の内部を、ストレージサブシステムにおいてフレーム毎に逐一判定して、フレーム内に格納された N\_Port\_Name がテーブル内に存在する場合にアクセスを許可し、存在しない場合は LS\_RJT という接続拒否のフレームを上位に対して送出することによ

って、前記テーブル内に存在しないN\_Port\_Nameをもつ上位装置からのアクセスを拒否するというものである。

#### 【0005】

【発明が解決しようとする課題】しかし上記方法では、第一に接続可否の判定をフレーム毎に行う必要があるために通信性能が大幅に制限されること、第二にアクセス可否の対象がポートではなくストレージサブシステム内の部分領域である場合、上位装置から送出されるフレームすべてにN\_Port\_Nameを格納することが上位装置に要求されるため、上位装置側に標準ファイバチャネルプロトコル範囲外の仕様の実装を強いることから、実際の製品に適用することは困難である。

【0006】本発明はANSI X3T11で標準化されたファイバチャネルプロトコルを上位装置とのインタフェースとしてもつストレージサブシステムにおいて、上位装置からストレージサブシステム内の記憶領域へのアクセスを選択的に制限することにより、不正アクセスを防止することを目的とする。

【0007】またこの際、アクセスの可否を判定する際生じるオーバーヘッドが最小限となる方法を提供し、かつ判定の条件を標準ファイバチャネルプロトコルの範囲のみで行える方法を提供することを目的とする。

#### 【0008】

【課題を解決するための手段】上記課題を解決するために、上位装置又は上位装置のポートを静的に一意に識別する識別手段であるN\_Port\_Name或いはNode\_Nameと、ストレージサブシステム内におけるアクセス可否判定の対象である各記憶領域とを対応づけたテーブルをストレージサブシステム内に保持し、さらにN\_Port\_Name或いはNode\_Nameと、上位装置がファイバチャネルインタフェースを用いてストレージサブシステムと通信を行う際に、上位装置又は上位装置のポートを一意に識別する手段として、情報の送受信に先立つログインプロセスにより動的に割り当てられる情報であるS\_IDとを関連付けたテーブルをストレージサブシステム内に保持し、上位装置からストレージサブシステム内の記憶領域に対する情報取得要求が、Inquiryコマンドを用いて行われた契機で、要求フレームに含まれるS\_IDを用いて、上記テーブルを検索及び比較することによって記憶領域に対するアクセス可否を判定する。

#### 【0009】

【発明の実施の形態】以下、本発明の実施の形態について、図を用いて詳細に説明する。まず、本発明で使用するファイバチャネルの特徴について説明する。

【0010】ファイバチャネルは、独自のコマンドセットを持たないシリアルな転送方式をもつプロトコルであり、情報を非同期に送るために伝送媒体の帯域幅を有効に利用できる特色を持っている。そして独自のコマンドセットを持たないかわりに、物理転送方式を、従来のSCSI、ESCONといったコマンドセットの運搬路として使用

することにより、従来のソフトウェア資産を継承しながら、より高速かつ多彩なデータ転送を可能としている。

【0011】ファイバチャネルはチャネルとネットワークの特長を併せ持つインタフェースである。すなわち、ファイバチャネルでは一旦転送元と転送先が確定すれば、遅延が少ない高速な転送が行える。これはチャネルの特長である。また、通信を希望する機器は、任意の契機でファイバチャネルの通信系に参加し、通信の目的となる相手の機器と相互に情報を交換することにより、互いを認識して通信を開始することができる。これはネットワークの特徴である。ここで述べた相手の機器との情報交換の手続きを、とくにログインと呼ぶ。

【0012】ファイバチャネルのインタフェースを持つ機器をノードと呼び、実際のインタフェースにあたる部分をポートと呼ぶ。ノードは1つ以上のポートを持つことが可能である。ファイバチャネルの系全体に同時に参加できるポートの数は、最大で24ビットのアドレスの数すなわち約1677万個である。この接続を媒介するハードウェアをファブリックと呼ぶ。送信元及び送信先のポートは、ファブリックを意識せずに互いのポートに関する情報のみを考慮して動作すればよいので、ファブリックを論理的な媒体として議論する場合も多い。

【0013】各ノード及びポートには、標準化団体から一定のルールによって割り当てられる世界中でユニークな識別子が記憶されている。これはTCP/IPのMACアドレスに相当するものであり、ハードウェア的に固定なアドレスである。このアドレスにはN\_Port\_Name、Node\_Nameの2種類があり、それぞれ8バイトの領域を持つ。N\_Port\_Nameはポート毎に固有の値、Node\_Nameはノード毎に固有の値となる。

【0014】ファイバチャネルでは、通信はOrdered Setと呼ばれる信号レベルの情報と、フレームと呼ばれる固定のフォーマットを持った情報とで行われる。

【0015】図1はこのフレームの構造を示している。フレーム101は、フレームの始まりを示すSOF (Start of Frame) 102と呼ばれる4バイトの識別子、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ103、実際に転送される目的となるデータ部分であるデータフィールド104、4バイトの巡回冗長コード(CRC) 105、フレームの終わりを示すEOF (End of Frame) 106と呼ばれる4バイトの識別子からなる。データフィールド104は0~2112バイトの間で可変である。

【0016】次に、図2を用いてフレームヘッダの内容について説明する。図2はフレームヘッダの構造について示している。ここではフレームヘッダ202の詳細構造203における、1ワードの23-0ビット領域にあたるS\_ID204のみ説明する。S\_ID (Source ID) 204は当該フレームを送信するポートを識別するための3バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。そして上位装置を動的に一意に識別できる情報

であり、PLOGI時（後述）に上位装置より報告される値である。このS\_IDは動的に変動する値であり、FC\_PHではファブリックによって初期化手続き時に割り当てられることになっている。割り当てられる値は、それぞれのポートが持つN\_Port\_Name、Node\_Nameに依存する。

【0017】次に、送信元の機器と送信先の機器が互いに情報を交換する、ログイン手続きについて述べる。図3に、上位装置からストレージサブシステムへの通信要求であるPLOGIフレームの構造について示す。フレームヘッダ302の詳細構造304において、ワード1の23-0ビットがS\_ID306である。また、データフィールド303の詳細構造305において、先頭から21バイト目～29バイト目までの8バイトの領域がN\_Port\_Name307を格納する領域であり、先頭から30バイト目～38バイト目までの8バイトの領域がNode\_Name308を格納する領域である。

【0018】図4は、送信元（ログイン要求元）と送信先（ログイン要求先）との間に取り交わされる情報を示したものである。ファイバチャネルのログイン手続きには数種類があるが、ここではクラス3のログインで取り交わされる情報を示す。

【0019】ログイン要求元は、PLOGIフレーム403をログイン要求先へ送信する。このフレームには、ログイン要求元のN\_Port\_Name、Node\_Name、S\_ID及びその他の情報が含まれている。要求先の装置では、このフレームに含まれている情報を取り出し、ログインを受諾する場合はACC404と呼ばれるフレームをログイン要求元に対して送信する。

【0020】ログインを拒絶する場合は図5に示すように、PLOGIフレーム503に対して、ログイン受信先はLS\_RJT504と呼ばれるフレームをログイン要求元に対して送信する。

【0021】ログイン要求元は、自らが送信したPLOGIフレームに対するACCフレームの応答を受信すると、ログインが成功したことを知り、データ転送などのI/Oプロセスを開始できる状態となる。LS\_RJTを受信した場合はログインが成立しなかったため、ログイン要求先へのI/Oプロセスは不可となる。ここではクラス3のログインについて述べたが、他のログインにおいても、ログイン要求元からログイン要求先へ渡すことのできる情報の中に、N\_Port\_Name、Node\_Name及びS\_IDが含まれることは同様である。

【0022】次に、Inquiryコマンドについて説明する。Inquiryコマンドとは、I/Oプロセスを開始しようとする場合に先立ち、プロセスの対象となる論理デバイスに対して、その実装状態を問い合わせるコマンドである。例えば、上位装置からストレージサブシステムに含まれる記憶領域へのアクセス要求に先立つ情報問い合わせ要求のことである。本コマンドはSCSIでは必ずサポートされている標準コマンドである。

【0023】図6は、SCSI規格で定義されたInquiryコマ

ンドを、ファイバチャネル規格のフレームで送信する場合のフレーム601のフォーマットである。フレームヘッダ602の詳細構造604において、本フレームに先立つPLOGIで割り当てられたS\_ID605が含まれている。データフィールド603にはFCP\_LUN607、FCP\_CNTL608、FCP\_CDB609、FCP\_DL610と呼ばれる領域がある。ここではFCP\_LUN607、及びFCP\_CDB609について述べる。

【0024】FCP\_LUN607の中には、フレーム送信元が状態を問い合わせようとする、フレーム送信先のポートに関連付けられた論理ボリュームの識別子が格納されている。この識別子をLUNという。FCP\_CDB609の中には、SCSIコマンドセットを使用する場合にはSCSIのコマンド記述ブロック（CDB）と呼ばれる命令情報が格納される。このFCP\_CDB609の中に、SCSIのInquiryコマンド情報が格納されて、前述のFCP\_LUN607と共に、フレーム要求先へ情報が転送される。

【0025】次に、Inquiryコマンドを受信したフレーム要求先が、問い合わせへの応答としてフレーム送信元へ返信する情報について述べる。この情報をInquiryデータと言う。図7にInquiryデータの抜粋を示す。ここでは、Inquiryデータ701のうちクオリファイア702と、デバイス・タイプ・コード703の2つについて述べる。クオリファイア（Peripheral Qualifier）702は、指定された論理ユニットの現在の状態を設定する3ビットの情報である。

【0026】図8はビットパターンによって示される論理ユニットの状態を列挙したものである。コード000（2進）802は、論理ユニットとして接続されている装置がデバイス・タイプ・コード703の領域に示される種類の入出力機器であることを示している。本コードが設定されていても、その論理ユニットが使用可能、すなわちレディ状態であることを必ずしも示しているわけではないが、その論理ユニットを使用できる可能性があるのは本コードが設定されている場合に限る。

【0027】コード001（2進）803は、論理ユニットとして接続されている装置がデバイス・タイプ・コード703の領域に示される種類の入出力機器であることを示しており、かつそのロジカルユニットには実際の入出力機器が接続されていないことを示している。これは例えばCD-ROMドライブが実装されているが、CD-ROMがドライブ内に挿入されていないような場合を示すことになる。コード011（2進）804は、指定された論理ユニットがサポートされていないことを示す。従って指定された論理ユニットに装置が割り当てられることはない。本コードが設定されるときは、デバイス・タイプ・コード領域703にはかならず1F（16進）が設定されることが条件になっている。

【0028】デバイス・タイプ・コード（Peripheral Device Type）703は、指定された論理ユニットに実際に割り当てられている入出力機器の種別を示す5ビットの



情報である。

【0029】図9に各デバイスタイプ902に対応するに16進のコード901を示す。図9に示されている情報のうち、未定義又は未接続のデバイス903を表す1F (16進) 904が設定されると、Inquiryコマンド送信元が問い合わせたデバイスは未定義或いは未接続ということになり、当該論理ユニットは当該送信元からは使用できないことになる。

【0030】図10に、このInquiryコマンドを用いた論理ユニット問い合わせの手順を示す。論理ユニットにアクセスしようとする上位装置1001は、アクセスしようとする論理ユニットをもつストレージサブシステム1002に対し、Inquiryコマンドを含むフレーム1003を送信する。このフレームには、PLOGIで割り当てられた、上位装置のS\_IDと、問い合わせを行う論理ユニットの識別子であるLUNが含まれている。なおここで、LUNについては、FCP\_LUN領域の他に、FCP\_CDB内のInquiryコマンド情報そのものの中にも設定することができる。どちらの値を使用しても得られる効果は同じであるが、本実施例ではLUNの値はFCP\_LUNに格納された値を使用するものと

【0031】Inquiryコマンドを含むフレームを受信したストレージサブシステム1002は、問い合わせに対する返答に必要なInquiryデータを準備し、作成したInquiryデータを含むフレーム1004を上位装置に対して送信する。このときInquiryデータを格納するフレームを、FCP\_DATAと呼ぶ。このとき、ストレージサブシステムが、問い合わせのあったロジカルユニット（論理ユニット）について、クオリファイア000 (2進)、デバイスタイプ00~09 (16進) のいずれかを設定した場合、このInquiryデータを受信した上位装置は、ロジカルユニットに対するI/Oを試みる事が可能となる。

【0032】また、図11に示すように、ストレージサブシステム1102が、クオリファイア001 (2進) 又は011 (2進)、デバイスタイプ1F (16進) を設定した場合、このInquiryデータ1104を受信した上位装置は、ロジカルユニットに対するI/Oが不可能であることを検出する。これらのことから、Inquiryデータに格納するクオリファイア、及びデバイス・タイプ・コードを管理することによって、上位装置からのロジカルユニットへのアクセスの許可及び不許可を制御することが可能となる。

【0033】本発明では、上位装置からのアクセスを許可、或いは拒否する対象として、ストレージサブシステム内の一定領域を選択することを可能としている。この領域は上位装置から明示的にアドレス指定が可能な領域であり、LU (Logical Unit) と呼ばれる。LUの識別子をLUN (Logical Unit Number) と呼ぶ。SCSI-2ではLUNの個数は1ターゲットあたり8である。

【0034】次に、本発明による処理の流れについて説明する。

【0035】図12は、本発明の実施例となる装置の構成図である。本装置をストレージサブシステム1201と呼ぶ。ストレージサブシステム1201は、複数のファイバチャネルインタフェースを持つポート1202によって上位装置（ホストと呼ぶ）1203と接続されている。接続形態はファイバチャネル規約によりさまざまであるが、本発明では接続形態を問わないため一括してファイバチャネル1204として表記してある。

【0036】上位装置1203もまたファイバチャネルインタフェースを持つポート1205を1つ以上備えており、それぞれのポート1205がストレージサブシステム1201上のポート1202とファイバチャネルプロトコルにより通信可能である。

【0037】ストレージサブシステム1201は中央演算装置1206を持ち、各種処理を行う。またストレージサブシステム1201は内部に不揮発メモリ1207を備えている。この不揮発メモリ1207は各種テーブルやN\_Port\_Name或いはNode\_Nameを保持する保持手段としての役割を果たす。デバイスドライバ制御部1208はバス1209を介して情報を記憶しているドライブデバイスと接続されている。本図ではドライブデバイスを論理単位としてとらえ、論理ユニット (LU) 1210として表示している。

【0038】また、ストレージサブシステム1201は通信制御部1211を持ち、通信回線1212を介して保守用装置1213の通信制御部1214と情報の送受信を行うことができる。保守用装置1213とは例えばパソコンのようなものであり、中央演算装置1215と入力手段1216及び表示手段1217を持つ。ユーザはこの保守用装置1213を用いて、ストレージサブシステム1201の保守を行う他、N\_Port\_Name或いはNode\_NameとLU1210の特定の記憶領域とを関連付け上位装置1203に対するアクセス可否を定義した情報（アクセス可否テーブル）を設定する。このように保守用装置1213は設定手段の役割も果たす。不揮発メモリ1207はこのように定義したアクセス可否テーブルをN\_Port\_Name或いはNode\_Nameと共に保持する。

【0039】更に不揮発メモリ1207は、中央演算装置1215で作成する関連テーブル（上位装置1203からストレージサブシステム1201への通信要求であるPLOGIを受け付けた際に、N\_Port\_Name或いはNode\_Nameと上位装置1203とを動的に一意に識別できる情報であり、PLOGI時に上位装置1203より報告される値であるS\_IDとを関連付け、このS\_IDを不揮発メモリ1207内に保持してあるN\_Port\_Name或いはNode\_Nameと関連付けたテーブル）を保持する。

【0040】図13は、本発明によるLUNセキュリティの実現方法の概要を説明したものである。まず手順1301では、ユーザは予めホストが持つN\_Port\_Nameを用いて、ストレージサブシステムの各ポート毎に関連付けられたLUNと、そこにアクセスしうるホストのN\_Port\_Nameを結び付けたアクセス可否テーブルを保守用装置（図12参

照)などを用いて作成し、ストレージサブシステム内の記憶領域(図12に示す不揮発メモリ等)に保持する。ここで得られるN\_Port\_Nameは既知であるとする。

【0041】次に、手順1302において、ホストがストレージサブシステムに対してログインを行う。ストレージサブシステムは、このログインのPLOGIフレームからホストのN\_Port\_Name及びS\_IDを取り出し、N\_Port\_NameとS\_IDとを関連付けた関連テーブルを作成する。作成された関連テーブルは、先のアクセス可否テーブルと同様にストレージサブシステム内の記憶領域に保持される。

【0042】次に、手順1303に移り、ホストはストレージサブシステム内の論理ユニットの状態を検査するためにInquiryコマンドを送信する。このInquiryコマンドを受信したストレージサブシステムは、Inquiryコマンドを格納しているフレームのヘッダからS\_IDを取り出し、また同フレームからInquiryコマンドの対象となるLUNを取り出す。そして関連テーブルを使用して、S\_IDからN\_Port\_Nameを割り出し、さらにアクセス可否テーブルからそのLUNがN\_Port\_Nameに対してアクセス許可されているか、もしくは不許可であるかの情報を取得する。

【0043】許可か不許可かの情報を用いて手順1304で中央演算装置はアクセス可否の判定をおこなう。結果が許可であった場合は、手順1305においてInquiryデータにLUが実装であることを設定し、不許可であった場合は、手順1307においてInquiryデータにLUが未実装であることを設定し、ホストに対して送信する。Inquiryデータを受信したホストはデータを解析し、対象LUが実装である、すなわち対象LUへのアクセスが許可されていることをデータから得ると、手順1306に示すように、それ以降当該LUに対してのI/O要求を行うことが出来るようになる。

【0044】対象LUが未実装であることを検出すると、以降当該LUへのI/O要求へのI/O要求を行うことはできない。以上の手順により、ストレージサブシステム内のLUに対するセキュリティの管理が実現できたことになる。

【0045】尚、N\_Port\_Nameの代わりにNode\_Nameを用いた場合も同様である。また、アクセス可否の判断は中央演算装置ではなく、専用の処理装置を設けて判断手段としてもよい。

【0046】次に、各手順について詳細に説明する。

【0047】まず、最初の手順であるN\_Port\_NameとLUNとの対応づけを行うテーブル作成手順について説明する。

【0048】本発明におけるLUNに対するセキュリティ情報は、ストレージサブシステムに存在するポートを単位として管理されるものとする。つまり、論理ユニットLUは各ポートに対して定義され、ホストはこれらのポートを通してLUへアクセスする。したがって、セキュリティ情報もポート単位で管理されることになる。この場合必要な情報は、ホストを一意に特定できる情報、各LUの

識別子であるLUN、及びLUNに対するアクセスの可否を示す状態ビットである。

【0049】ホストを一意に特定できる情報とは、この時点ではN\_Port\_Nameとなる。N\_Port\_Nameは、ホストに存在するポート毎にユニークな値であるので、本発明によればホストのポート毎に、ストレージサブシステムのポートにおけるLUに対するセキュリティを設定できることになる。N\_Port\_Nameの替わりに、Node\_Nameを使用したテーブルを作成すれば、ホスト毎にセキュリティを設定することになる。LUに対するアクセス権限を与える対象がホストのポート毎であるか、ホスト毎であるかの相違であるので、本実施例ではN\_Port\_Nameについて説明する。すなわち本実施例ではホストのポート毎にセキュリティを設定する方法を述べるが、N\_Port\_Nameの記述をNode\_Nameに読み替えることによって、容易にホスト単位のセキュリティ設定方式を得ることができる。また、本実施例では、ホスト上にあるポートのことを、簡略化のためにホストと呼ぶことにする。つまり、ホストという語はホストそのものと、ホスト上に存在するポートの双方、或いはいずれかを意味することになる。

【0050】図14に、本実施例で作成するアクセス可否テーブルを示す。本テーブルはストレージサブシステム上にあるポート毎に作成される。作成はストレージサブシステムと通信可能な保守用の装置から、入力手段とその入力結果を確認するための表示手段を用いて指示することにより行う。通信回線の種類により、LANを用いればストレージサブシステムに近い場所からの設定、電話回線を用いれば保守センタ等遠隔地からの設定が可能である。また内部バスを用いて保守用装置とストレージサブシステムを一体化させることも可能である。

【0051】LUN1402はポートに関連付けられたLUを示し、N\_Port\_Name1403の数はそのポート配下に存在するLUへアクセスする可能性のあるホストの数だけ存在する。LU及びホストの数は有限な数となる。テーブルの各要素において、本実施例では値“1”がアクセス許可を、値“0”がアクセス拒否を意味することにする。図14では当該ポートにおいて、LUN 0へアクセス許可があるホストは、N\_Port\_Name “0123456789ABCDEF” 1409 をもつホストのみであり、LUN 1 1405へアクセス許可があるホストは、N\_Port\_Name “01234567 89ABCDEE” 1410及び “01234567 89ABCDEE” 1411をもつホストである。またLUN n-1 1407へのアクセスが許可されているホストは存在しない。

【0052】図15に示すように、本テーブルは、セキュリティの設定が必要なポートすべてについて作成し、ストレージサブシステム内の記憶領域に保持する。このとき記憶領域に不揮発記憶領域を使用すれば、ストレージサブシステムの電源が切断された場合でも情報を保持することができる。また、初期値を0又は1としてテーブルを作成しておくことにより、テーブル作成を簡略化する

ことができる。

【0053】次に、ホストからのログインの手順について詳細に説明する。本手順ではPLOGIに伴う情報から、ホストのN\_Port\_NameとホストのS\_IDを結び付ける処理を行う。

【0054】まず、図16の手順1602に示すように、ホストからのログイン手続きとして、PLOGIフレームが送信される。手順1603においてストレージサブシステムでは、PLOGIフレームのヘッダから、ホストのS\_IDを取得する。また同時に、手順1604において、PLOGIフレームのデータ領域から、ホストのN\_Port\_Nameを取得する。手順1605において、この2つの値を結び付け、図17に示すような関連テーブルを作成する。PLOGIはホストのポートと、ストレージサブシステム上のポートとの間で交

わされるログインであるので、本テーブルもストレージサブシステムのポート毎に作成されることになる。

【0055】手順1606でテーブルを更新することによって、本テーブルを用いて、S\_ID1701が与えられれば該当するN\_Port\_Name1702を得ることが可能となる。本テーブルも、ストレージサブシステム内の記憶領域に保持されることは図14で示したテーブルと同様である。ホストに対しては、手順1607でPLOGIに対する応答としてACCと呼ばれるフレームを送信し、ホストにログインが受理されたことを通知する。ACCフレームを受信したホストは、以降当該ポートに対してのInquiry等を発行することができるようになる。

【0056】次に、ホストからのInquiryコマンドの送信と、それに伴うセキュリティの応答について図18を用いて詳細に説明する。Inquiryコマンドは、FCP\_CMNDと呼ばれる情報単位を含むフレームとしてホストからストレージサブシステムへ送信される。手順1802でホストからのデータフィールド内のFCP\_CMNDフレームを受信したストレージサブシステムは、手順1803でFCP\_CMNDフレームの内容を解析する。FCP\_CMNDがInquiryコマンドでない場合は、それぞれに応じた処理1805に分岐する。FCP\_CMNDがInquiryコマンドであった場合は、手順1806に遷移し、当該フレームからS\_IDを切り出す。また、同時に手順1807にてFCP\_LUNからInquiryが対象としているLUNを取り出す。

【0057】次に、手順1808に移り、フレームから切り出したS\_IDから、図17で示したテーブルを用いてN\_Port\_Nameを求める。さらに、求めたN\_Port\_Nameについて、図14で示したテーブルより、Inquiryコマンドが対象としているLUNについて、セキュリティを示したビットの状態を取得する。この時ホストから得られたS\_IDが、FF FF01であり、Inquiryの要求するLUNが0であったとする。まず手順1808にて、図17に示すテーブルよりS\_ID FF FF01 1703に対応するN\_Port\_Name “01234567 89ABCDEF” 1706 を取得した後、手順1809に移り図14に示したテーブルよりN\_Port\_Name “01234567 89ABCDEF” 1409 に対す

るLUN 0 1404のセキュリティ “1” を得る。

【0058】セキュリティ “1” は本実施例ではアクセス許可を意味するので、手順1811に分岐し、ホストへ報告するInquiryデータとして、クオリファイアに000 (2進)、デバイスタイプに当該デバイスに対応するコードをセットする。例えばストレージサブシステムがハードディスクアレイサブシステムである場合は、デバイスタイプは00 (16進) となる。ついでInquiryデータを格納したフレームを作成し、手順1813でホストに対して送信をおこなう。さらに手順1814にて、返信が終了したことを示すFCP\_RSPと呼ばれるフレームをホストに対して送信する。

【0059】この一連の返信データを受け取ったホストは、Inquiryの結果として当該LUN=0のLUに対してアクセスができることを検知したことになるため、以降は次回

のInquiryコマンドを受け付けるまで、当該LUに対してセキュリティのチェックを行う必要なくアクセスを行うことが可能となる。

【0060】次にアクセスを拒否する場合を説明する。Inquiryコマンドの送信によりホストから得られたS\_IDがFFFF01であり、Inquiryの要求するLUNが1であったとする。手順1808において、図17に示す関連テーブルよりS\_ID FFFF01 1703に対応するN\_Port\_Name “01234567 89ABCDEF” 1706を取得した後、図14に示すアクセス可否テーブルよりN\_Port\_Name “01234567 89ABCDEF” 1409に対するLUN 1 1405のセキュリティ “0” を得る。

【0061】セキュリティ “0” は本実施例ではアクセス拒否を意味するので、手順1812へ分岐し、ホストへ報告するInquiryデータとして、クオリファイアに001 (2進) 又は011 (2進)、デバイス・タイプ・コードに1F (16進) をセットしたInquiryデータを作成する。このInquiryデータを受信し、ついでFCP\_RSPを受信したホストは、Inquiryの結果として当該LUN=1のLUが未実装であるという情報を得る。したがって、以降ホストは当該LUが実装されていないと判断するのでアクセス要求をすることはなくなる。

【0062】以上のようにして、N\_Port\_Name、S\_ID、LUNを用いたテーブルを保持することで、ストレージサブシステム側のポート毎に、ホストの各ポートに対しての各LUNへのアクセスについてのセキュリティを、ログイン及びInquiryの際に判断することで、効率よく行うことができる。

#### 【0063】

【発明の効果】本発明によって、上位装置から特定LUNに対するアクセスを、予め設定してあるN\_Port\_Name或いはNode\_NameとLUNとのアクセス可否テーブル、PLOGIの際に判明するN\_Port\_Name或いはNode\_NameとS\_IDとの関係を用いて作成した関連テーブルの双方のテーブルを用いることによって、上位装置或いは上位装置のポートからのLUへの状態問い合わせがあった時点でアクセス可

否を決定し返答することができるため、ストレージサブシステムへのアクセス制限を、LUN単位で、しかも初回のみの判定プロセスで行うことができ、ファイバチャネル及びSCSIの規格上最も分解能の高いセキュリティを、高いパフォーマンスで確保することができる。

#### 【図面の簡単な説明】

【図1】ファイバチャネルプロトコルにおけるフレームの構造図である。

【図2】フレームヘッダの構造図である。

【図3】PLOGIフレームの構造図である。

【図4】PLOGIが受諾されるシーケンス図である。

【図5】PLOGIが拒否されるシーケンス図である。

【図6】SCSIのInquiryコマンドを含むフレームの構造図である。

【図7】Inquiryデータの構造図である。

【図8】Inquiryデータ中クオリファイアの内容定義図である。

【図9】Inquiryデータ中デバイス・タイプ・コードの内容定義図である。

【図10】InquiryデータにLU通常状態が設定される場合のシーケンス図である。

【図11】InquiryデータにLU未定義状態が設定される場合のシーケンス図である。

【図12】ストレージサブシステムの構成図である。

【図13】全体シーケンスのフローチャートである。

【図14】N\_Port\_Nameに対するLUアクセス可否の定義テーブルである。

【図15】LUアクセス可否定義テーブルの設定フローチャートである。

【図16】PLOGI処理のフローチャートである。

【図17】ホストN\_Port\_NameとS\_IDを関連付けるテーブルである。

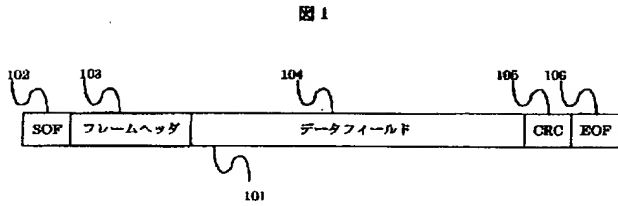
【図18】Inquiryコマンド処理のフローチャートである。

#### 【符号の説明】

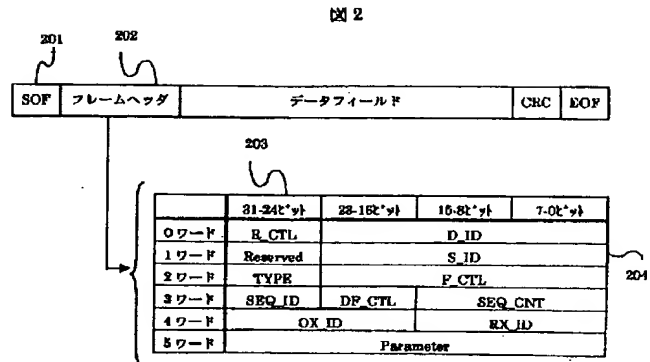
101…フレーム、102…SOF (Start of Frame)、103…フレームヘッダ、104…データフィールド、105…CRC、106…EOF (End of Frame)、201…フレーム、202…フレームヘッダ、203…フレームヘッダ詳細、204…S\_ID、301…フレーム、302…フレームヘッダ、303…データフィールド、304…フレームヘッダ詳細、305…データフィールド詳細、306…S\_ID、307…N\_Port\_Name、308…Node\_Name、401…ログイン要求元の動作、402…ログイン受信先の動作、403…PLOGIフレームの内容、404…ACCフレーム、501…ログイン要求元の動作、502…ログイン受信先の動作、503…PLOGIフレームの内容、504…LS\_RJTフレーム、601…フレーム、602…フレームヘッダ、603…デ

ータフィールド、604…フレームヘッダ詳細、605…S\_ID、606…データフィールド詳細 (FCP\_CMND)、607…FCP\_LUN、608…FCP\_CNTL、609…FCP\_CDB (Inquiry)、610…FCP\_DL、701…Inquiryデータ抜粋、702…クオリファイア、703…デバイス・タイプ・コード、801…クオリファイアの定義、802…000 (2進)、803…001 (2進)、804…011 (2進)、901…デバイス・タイプ・コード (16進)、902…デバイス・タイプ、903…1F (16進)、904未定義又は未接続のデバイス、1001…上位装置 (ホスト) のInquiry処理シーケンス、1002…ストレージサブシステムのInquiry処理シーケンス、1003…Inquiryを含むフレーム (FCP\_CMND) に格納される情報、1004…デバイス通常状態を通知するInquiryデータ、1101…上位装置 (ホスト) のInquiry処理シーケンス、1102…ストレージサブシステムのInquiry処理シーケンス、1103…Inquiryを含むフレーム (FCP\_CMND) に格納される情報、1104…デバイス未定義状態を通知するInquiryデータ、1201…ストレージサブシステム、1202…ストレージサブシステムのファイバチャネルポート、1203…上位装置 (ホスト)、1204…ホストとストレージサブシステムを接続するファイバチャネルプロトコル、1205…ホストのファイバチャネルポート、1206…中央演算装置、1207…不揮発メモリ、1208…デバイスドライブ制御部、1209…バス、1210…LU (論理ユニット)、1211…通信制御部、1212…通信回線、1213…保守用装置、1214…通信制御部、1215…中央演算装置、1216…入力手段、1217…表示手段、1301…全体手順1、1302…全体手順2、1303…全体手順3、1304…全体手順4、1305…全体手順5、1306…全体手順6、1307…全体手順7、1401…N\_Port\_Nameに対するLUアクセス可否定義テーブル、1402…LUN、1403…N\_Port\_Name、1404…LUN 0のLUに対する定義、1405…LUN1のLUに対する定義、1406…LUN 2のLUに対する定義、1407…LUN n-1のLUに対する定義、1408…LUN nのLUに対する定義、1409、1410、1411…N\_Port\_Name、1601…PLOGI処理フローチャート開始、1602…PLOGI処理手順1、1603…PLOGI処理手順2、1604…PLOGI処理手順3、1605…PLOGI処理手順4、1606…PLOGI処理手順5、1607…PLOGI処理手順6、1701…S\_ID、1702…N\_Port\_Name、1703、1704、1705…S\_ID、1706、1707、1708…N\_Port\_Name、1801…Inquiry処理フローチャート開始、1802…Inquiry処理手順1、1803…Inquiry処理手順2、1804…Inquiry処理手順3、1805…Inquiry処理手順4、1806…Inquiry処理手順5、1807…Inquiry処理手順6、1808…Inquiry処理手順7、1809…Inquiry処理手順8、1810…Inquiry処理手順9、1811…Inquiry処理手順10、1812…Inquiry処理手順11、1813…Inquiry処理手順12、1814…Inquiry処理手順13。

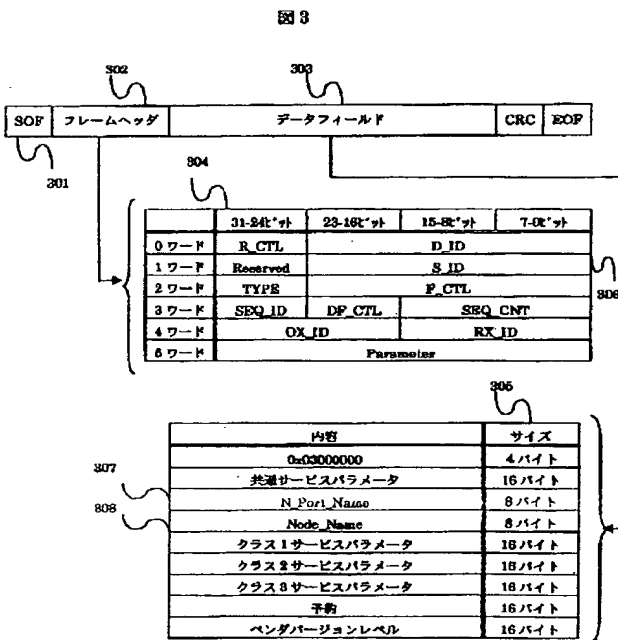
【図 1】



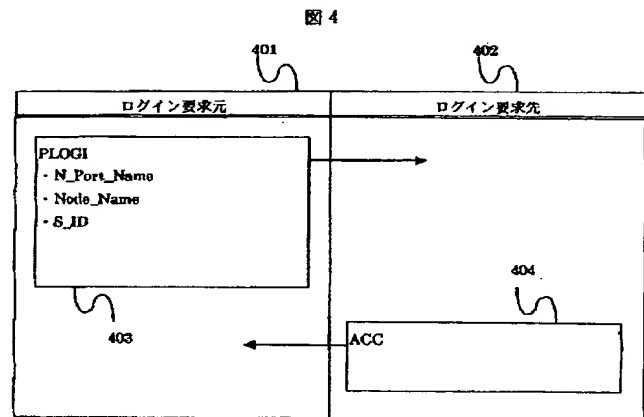
【図 2】



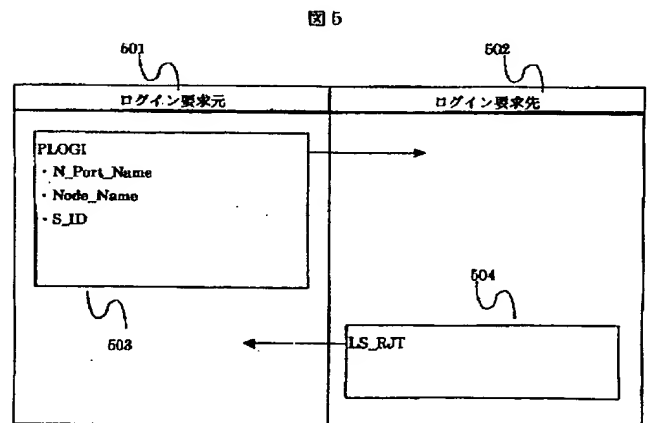
【図 3】



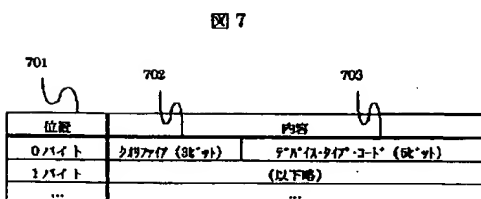
【図4】



【図 5】

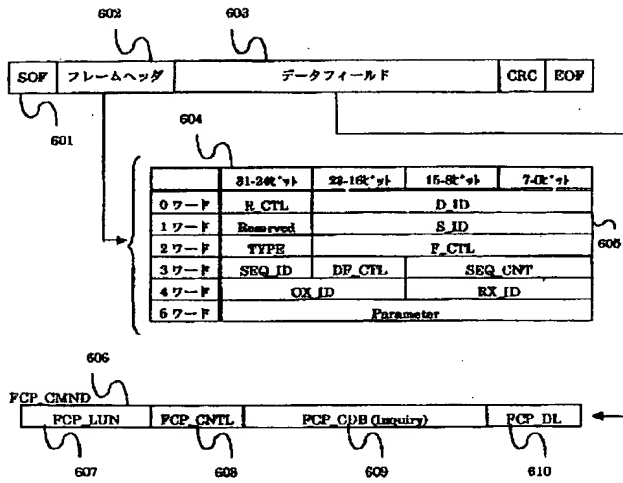


【图 7】



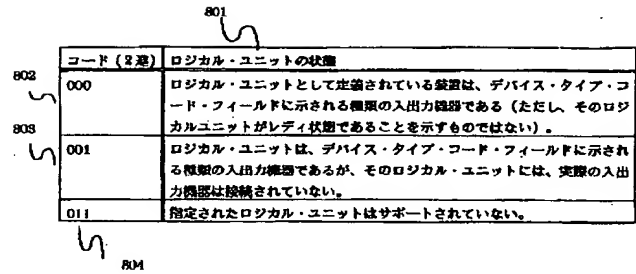
【図 6】

図 6



【図 8】

図 8



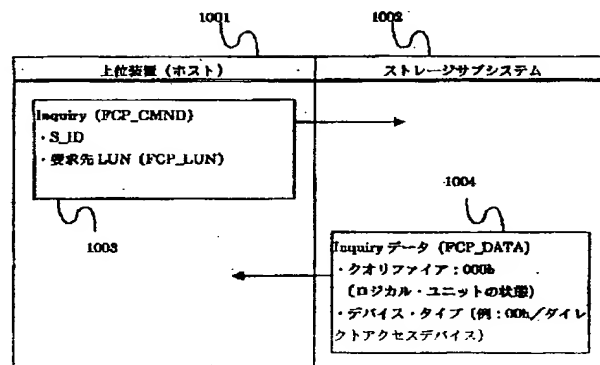
【図 9】

図 9

コード (16進)	デバイス・タイプ
00h	ダイレクト・アクセス・デバイス (例: 磁気ディスク)
01h	シーケンシャル・アクセス・デバイス (例: 磁気テープ)
02h	プリンタ・デバイス
03h	プロセッサ・デバイス
04h	ライト・ワンス・デバイス (例: 追記型光ディスク)
05h	CD-ROM デバイス
06h	スキャナ・デバイス
07h	光メモリ・デバイス (例: イレーザブル光ディスク)
08h	メディア・チェンジャ・デバイス (例: 磁気テープ (または光ディスク) ライブラリ)
09h	コミュニケーション・デバイス (例: 通信回線)
0Ah~0Bh	(グラフィック装置用に定義予定)
0Ch~1Eh	(リザーブ)
1Fh	未定義または未接続のデバイス

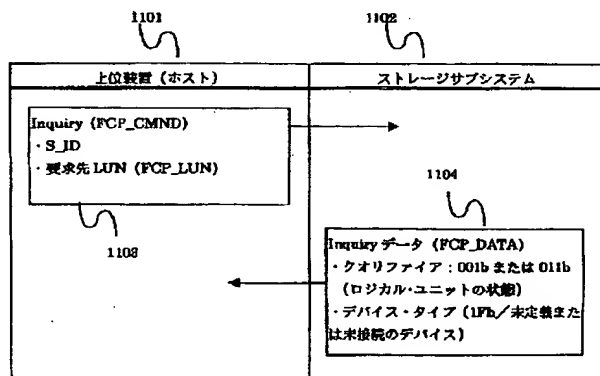
【図 10】

図 10



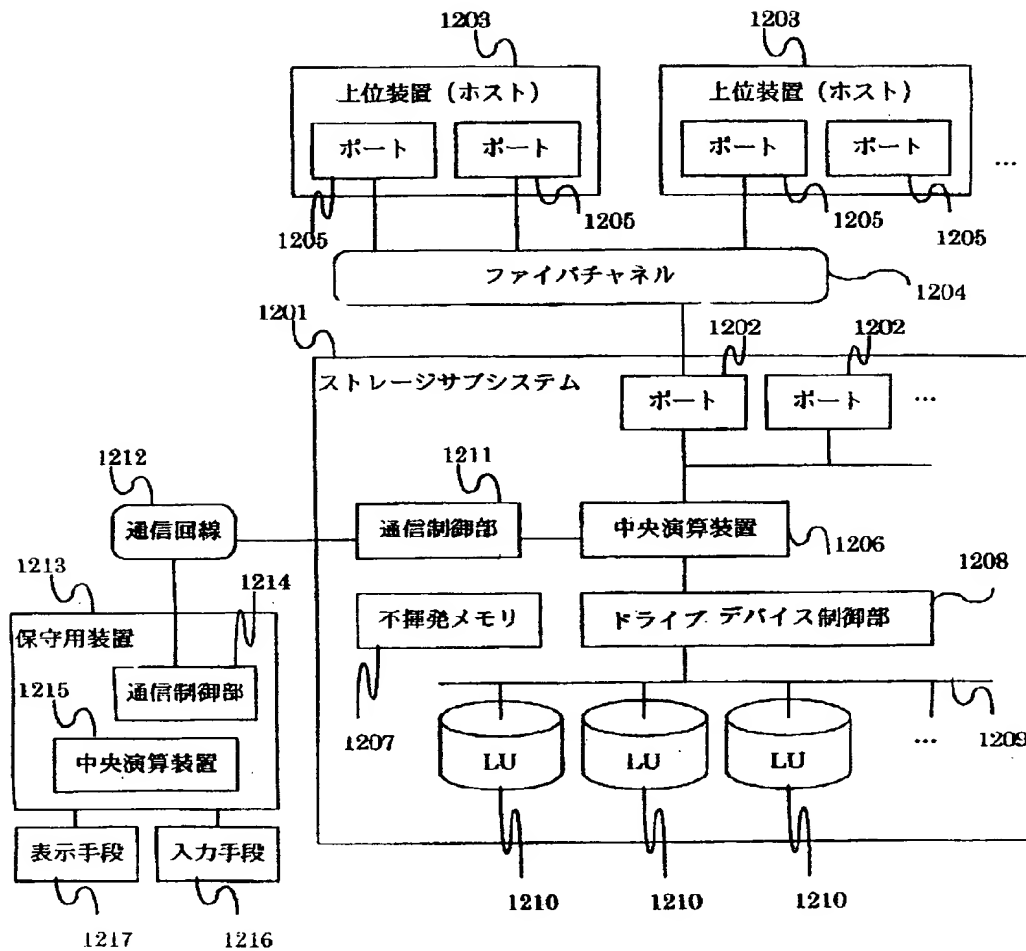
【図 11】

図 11



【図 12】

図 12



【図 14】

図 14

LUN						N_Port_Name	
0	1	2	...	n-1	n	01234567 89ABCDEF	1409
1	0	0	...	0	0	01234567 89ABCDEE	1410
0	1	0	...	0	1	01234567 89ABCDDE	1411
0	1	1	...	0	1	01234567 89ABCDDE	
...	...	...	...	...	...	...	

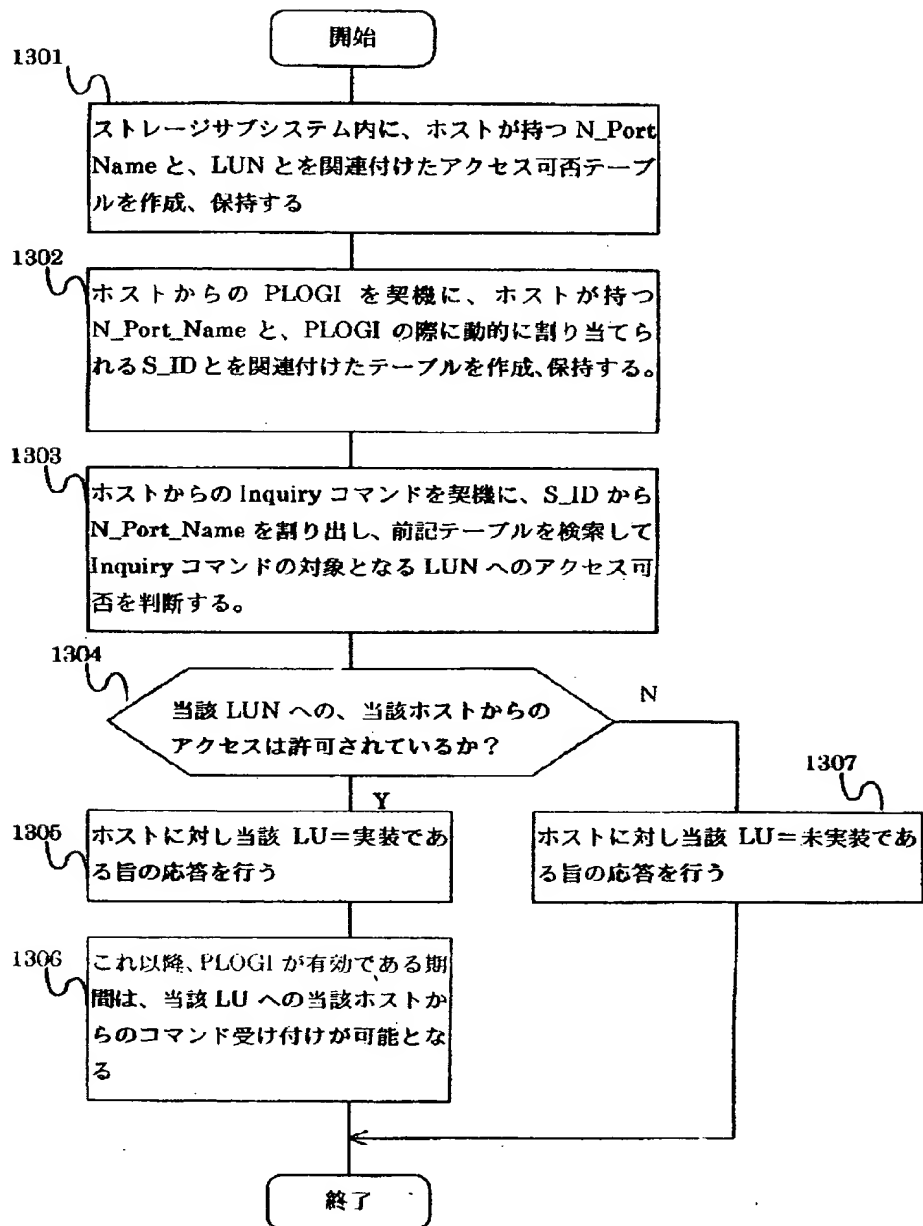
【図 17】

図 17

S_ID	N_Port_Name
FFFF01	01234567 89ABCDEF
FFFF02	01234567 89ABCDEE
FFFF03	01234567 89ABCDDE
...	...

【図 13】

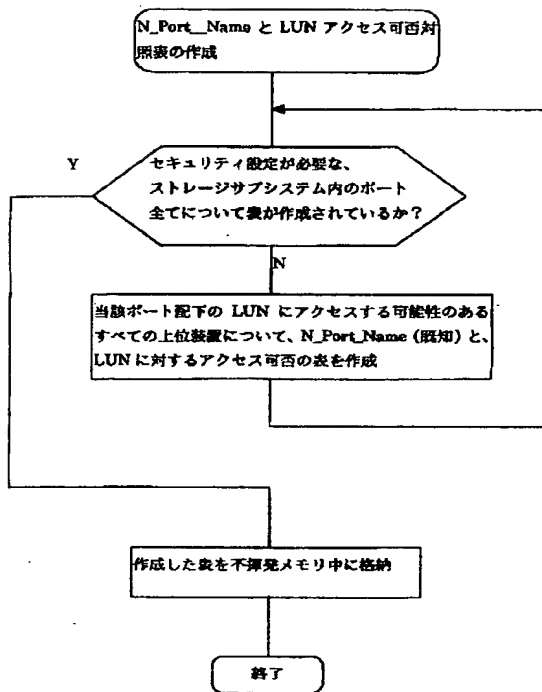
図 13





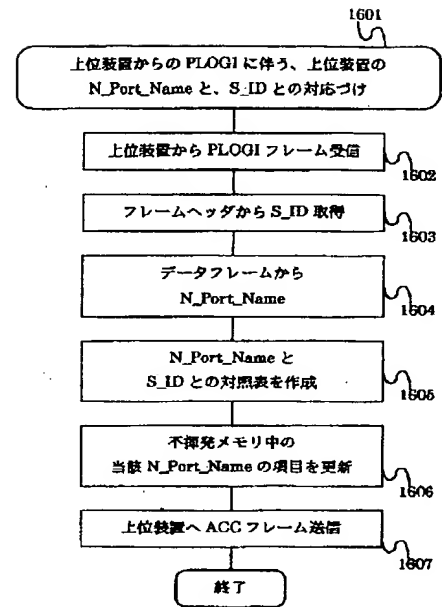
【図 15】

図 15



【図 16】

図 16



【図 18】

図 18

